

### **Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

### **Listing of Claims:**

Claim 1 (previously presented): A communication switch comprising:  
at least one input to receive messages, each message including,  
an address specifier, and  
a port specifier;  
a traffic analyzer to compare the port specifier of a first message against port specifiers of  
previously received messages; and  
an output to report a result of the comparison to a remote location.

Claim 2 (currently amended): The communication switch of claim 1 further comprising:  
a usage tracking system to throttle traffic through the communication switch to/from a  
device associated with a common address specifier and port specifier.

Claim 3 (currently amended): The communication switch of claim [[2] 1 wherein:  
the usage tracking system to throttle traffic based on a number of messages having ~~the~~  
~~same~~ a common address specifier and port specifier.

Claim 4 (currently amended): The communication switch of claim 2 wherein:  
the usage tracking system to throttle traffic according to a predetermined maximum  
aggregate bandwidth for the communication switch, the predetermined maximum aggregate  
bandwidth received from the remote location.

Claim 5 (currently amended): The communication switch of claim 1 wherein:  
the traffic analyzer to report fraud over the output to a service provider at the remote  
location.

Claim 6 (previously presented): The communication switch of claim 1 wherein:  
the traffic analyzer to compare the address specifier and port specifier combination of the  
first message against the address specifier and port specifier combinations of the previously  
received messages.

Claim 7 (previously presented): The communication switch of claim 1 wherein:  
each message further includes,  
a traffic type specifier; and  
the traffic analyzer is further to compare the traffic type specifier of the first message  
against traffic type specifiers of the previously received messages.

Claim 8 (previously presented): The communication switch of claim 1 wherein:  
each message further includes,  
a traffic type specifier; and  
the traffic analyzer is further to compare the address specifier, port specifier, and traffic  
type specifier of the first message against address specifier, port specifier, and traffic type  
specifier combinations of the previously received messages and to report information to the  
remote location regarding a combination of request types originating from the same address  
specifier and port specifier.

Claims 9-12 (canceled)

Claim 13 (previously presented): A method comprising:  
receiving a first message which includes an address:port identifier;  
comparing the address:port identifier against previously received messages' address:port  
identifiers; and  
determining whether excessive traffic is originating from a source identified by a  
common address:port identifier of the first message and at least some of the previously received  
messages.

Claim 14 (original): The method of claim 13 further comprising:  
throttling message traffic in response to determining that excessive traffic is originating  
from the source.

Claim 15 (previously presented): The method of claim 14 wherein the throttling  
comprises:  
throttling message traffic to and/or from the source.

Claim 16 (previously presented): The method of claim 13 wherein the first message further includes a type specifier, the method further comprising:

comparing the type specifier against type specifiers of previously received messages having the same address:port identifier as the first message; and  
determining whether the source is issuing messages of different types.

Claim 17 (currently amended): The method of claim 16 further comprising:  
sending a fraud alert to a remote location in response to determining that the source is issuing messages of different types.

Claim 18 (previously presented): The method of claim 13 further comprising:  
recording the first message for use in future comparisons against future messages.

Claim 19 (original): The method of claim 13 further comprising:  
receiving an indication of a maximum bandwidth for a customer premises from a remote service provider; and  
throttling message traffic to/from the customer premises in response to the indication of the maximum bandwidth.

Claim 20 (currently amended): A customer premises gateway comprising:  
at least one first input/output (I/O) each to connect to a communication device;  
a second I/O to connect to an Internet service provider (ISP) premises head-end server;  
and  
a traffic analyzer coupled to the at least one first I/O and the second I/O, including  
a port identifier comparator,  
a throttling mechanism, and  
a fraud reporter to report excessive traffic from a common address identifier and port identifier combination of the communication device.

Claim 21 (original): The customer premises gateway of claim 20 wherein the traffic analyzer further includes:  
a message type analyzer.

Claim 22 (original): A machine accessible medium including therein instructions which, when executed by the machine, cause the machine to:

compare a first address:port combination of a message against a second address:port combination of a previously received message; and

responsive to the address:port comparison, determine whether excessive traffic is going to/from the first address:port combination.

Claim 23 (currently amended): The machine accessible medium of claim 22 further including therein instructions which, when executed by the machine, cause the machine to further:

throttle traffic to/from the first address:port combination based on the determination of excessive traffic.

Claim 24 (currently amended): The machine accessible medium of claim 23 further including therein instructions which, when executed by the machine, cause the machine to further:

report fraud to a service provider at a remote location.

Claim 25 (original): The machine accessible medium of claim 22 further including therein instructions which, when executed by the machine, cause the machine to further:

compare a first type specifier of the message against a second type specifier of the previously received message; and

responsive to the type specifier comparison, determine whether the first address:port identifies a router performing address:port masquerading.

Claim 26 (currently amended): The machine accessible medium of claim 25 further including therein instructions which, when executed by the machine, cause the machine to further:

report the masquerading to a service provider at a remote location.

Claim 27 (previously presented): A method comprising:  
receiving in a communication switch a message from a device, the message including address and sub-address identifiers;

comparing the address and sub-address identifiers against one or more previously received messages; and

determining whether the device is performing masquerading based on the comparison.

Claim 28 (previously presented): The method of claim 27 wherein the determining comprises:

observing a first message type indicator in the message and a different message type indicator in at least one of the previously received messages.

Claim 29 (original): The method of claim 27 further comprising:  
recording the address and sub-address identifiers of the message;  
receiving a second message; and  
comparing the second message's address and sub-address identifiers against the recorded address and sub-address identifiers.

Claim 30 (original): The method of claim 27 wherein:  
the address identifier comprises an Internet Protocol address; and  
the sub-address identifier comprises a port number.

Claim 31 (currently amended): The method of claim 27 further comprising:  
responsive to determining the masquerading, sending a fraud alert to a server associated with a service provider.

Claim 32 (previously presented): The method of claim 27 further comprising:  
throttling message transmission if the determining is indicative of masquerading.

Claim 33 (currently amended): The method of claim 27 further comprising:  
comparing a message type identifier of the message against one or more previously received messages; and  
detecting that the message type identifier of the message is different than a message type identifier of a previously received message having a same address identifier and a same sub-address identifier as the message; and  
communicating an alert based on the detecting to a remote service provider.

Claim 34 (canceled)

Claim 35 (new): The communication switch of claim 1, wherein the communication switch is to be coupled to a router at a customer premises, wherein a plurality of systems are to be coupled to the router at the customer premises.

Claim 36 (new): The communication switch of claim 4, wherein the predetermined maximum aggregate bandwidth is based on a bandwidth associated with a customer premises including the communication switch.